WHAT IS CLAIMED IS:

1. A client-server security system comprising:.

a client system receiving first biometric data and having a first level security authorization procedure; and

a server system receiving second biometric data and having a second level security authorization procedure;

wherein the first level security authorization procedure and the second level security authorization procedure comprise distinct biometric algorithms.

2. The client-server security system of claim 1 wherein the first biometric data comprises speech data.

3. The client-server security system of claim 2 wherein the speech data comprises to a password.

4. The client-server security system of claim 1 wherein the second biometric data comprises speech data.

5. The client-server security system of claim 1 wherein the first level of security authorization comprises user verification.

6. The client-server security system of claim 1 wherein the second level of security authorization comprises user identification.

7. The client-server security system of claim 1 wherein the first level of security authorization comprises a neural network.

8. The client-server security system of claim 1 wherein the second level of security authorization comprises Hidden Markov Models.

9. A method of performing a secured transaction on a server system comprising:

receiving a first level security authorization signal on the server system from a client system;

receiving biometric data on the server system from the client system;

executing a second level security authorization, the second level security authorization including analyzing the biometric data using a first biometric algorithm on the server system; and

generating a second level security authorization signal on the server system when the first biometric algorithm indicates that the biometric data corresponds to one of a plurality of users authorized to access the server system.

10. The method of claim 9 wherein the first level security authorization signal indicates that a user has been authorized on the client system by a second biometric algorithm on the client system.

11. The method of claim 9 wherein the first level security authorization signal indicates that a user has not been authorized on a client system by a second biometric algorithm on the client system.

12. The method of claim 9 further comprising re-executing the second level security authorization on the server system.

13. The method of claim 9 further comprising receiving control information from the client system.

14. The method of claim 13 wherein the control information comprises a verification confidence value.

15. The method of claim 14 further comprising modifying an acceptance threshold of the first biometric algorithm in accordance with the verification confidence value.

16. The method of claim 14 further comprising analyzing second biometric data using the first biometric algorithm when the verification confidence value within a first range.

17. The method of claim 14 further comprising prompting the user for additional biometric information when the verification confidence value is within a first range.

18. The method of claim 13 wherein the control information comprises a authorization limitation criteria.

19. The method of claim 18 further comprising restricting access to remote resources in accordance with the authorization limitation criteria.

20. The method of claim 18 further comprising limiting allowable spending amounts in accordance with the authorization limitation criteria.

21. The method of claim 18 further comprising limiting allowable network connection time in accordance with the authorization limitation criteria.

22. The method of claim 9 further comprising providing access to a plurality of server resources in accordance with the first and second level authorization signals.

23. The method of claim 9 further comprising providing access to a plurality of remote network resources in accordance with the first and second level authorization signals.

24. The method of claim 9 further comprising executing an identification script to obtain identification information about the user.

25. The method of claim 9 further comprising retrieving biometric data from the client and storing the biometric data on the server for later identification of the user.

26. The method of claim 25 wherein the biometric data is a digital fingerprint.

27. The method of claim 25 wherein the biometric data is a digital voice print.

28. The method of claim 9 further comprising receiving a line quality measure in the server system, and in accordance therewith, selecting one of a plurality of server biometric algorithms for executing the second level security authorization.

29. The method of claim 9 further comprising receiving a line quality measure in the server system, and in accordance therewith, loading the first biometric

algorithm with a first input parameter value when the line quality measure is in a first range, and loading the first biometric algorithm with a second input parameter value when the line quality measure is in a second range.

30. The method of claim 9 further comprising receiving a channel type signal in the server system, and in accordance therewith, loading the first biometric algorithm with a first input parameter value when the channel type has a first value, and loading the first biometric algorithm with a second input parameter value when the channel type has a second value.

31. A method of performing a secured transaction on a client system comprising:

receiving biometric data in the client system;

analyzing a first portion of the biometric data using a first biometric algorithm on the client system;

generating a first level security authorization signal on the client system when the first biometric algorithm indicates that the first portion of the biometric data corresponds to an authorized user;

transmitting the first level security authorization signal and second portion of the biometric data to a server system, the second portion of biometric being analyzed by a second biometric algorithm on the server; and

accessing resources on the server system through the client system when the second biometric algorithm provides a second level security authorization.

32. The method of claim 31 further comprising generating a verification confidence value and transmitting the verification confidence level to the server system.

33. The method of claim 32 further comprising modifying an acceptance threshold of the second biometric algorithm in accordance with the verification confidence value.

34. The method of claim 32 further comprising transmitting second biometric data to the server system and analyzing the second biometric data using the second biometric algorithm when the verification confidence value is within a first range.

35. The method of claim 31 further comprising generating authorization limitation criteria and transmitting the authorization limitation criteria to the server system.

36. The method of claim 35 wherein the authorization limitation criteria comprises remote resource access restrictions.

37. The method of claim 35 wherein the authorization limitation criteria comprises spending amount limitations.

38. The method of claim 31 wherein the first portion of the biometric data is speech data and the first biometric algorithm is a speaker recognition algorithm.

39. The method of claim 38 wherein the speech data comprises a password.

40. The method of claim 31 wherein the second portion of the biometric data is speech data and the second biometric algorithm is a speaker recognition algorithm.

41. The method of claim 40 wherein the speech data comprises an utterance.

42. The method of claim 31 wherein client system is a portable media player.

43. The method of claim 31 wherein client system is a smart card.